Centro de Especializaciones Noeder

Florida Global University

Diplomado de Especialización

IMPLEMENTADOR Y AUDITOR INTERNO DE CONTINUIDAD DEL NEGOCIO ISO 22301

CICLO INTENSIVO

MÓDULO II

RIESGOS Y AMENAZAS DE LA CONTINUIDAD DEL NEGOCIO

Ing. Johnattan Sifuentes Rojas

MODULO II – RIESGOS Y AMENZAS DE LA CONTINUIDAD DEL NEGOCIO

CONTENIDO MODULO II

1. Definiciones, Conceptos e Identificación de Riesgos y Amenazas.
2. Planificación y Operación de los riesgos en la Continuidad de Negocio
3. Análisis y evaluación de riesgos de Continuidad del Negocio
4. Determinación de criterios de riesgo
5. Tratamiento del riesgo
6. Aceptación del riesgo
7. Relación entre riesgos, controles y objetivos del SGCN

DEFINICIONES E IDENTIFICACION DE RIESGOS Y AMENAZAS

DEFINICIONES E IDENTIFICACION DE RIESGOS Y AMENAZAS

RIESGO – ISO 22301

Riesgo

Efecto de incertidumbre sobre los objetivos

Apetito por el Riesgo

Cantidad y tipo de riesgo que una organización está dispuesta a conseguir o conservar

Evaluación de Riesgos

Proceso general de identificación, análisis evaluación de riesgos

Gestión de Riesgos

Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo

DEFINICIONES E IDENTIFICACION DE RIESGOS Y AMENAZAS

ISO 22399

Probabilidad

Grado al que es probable que se produzcan un evento

Consecuencia

Resultado de un evento

Impacto

Consecuencia evaluada de un resultado en particular

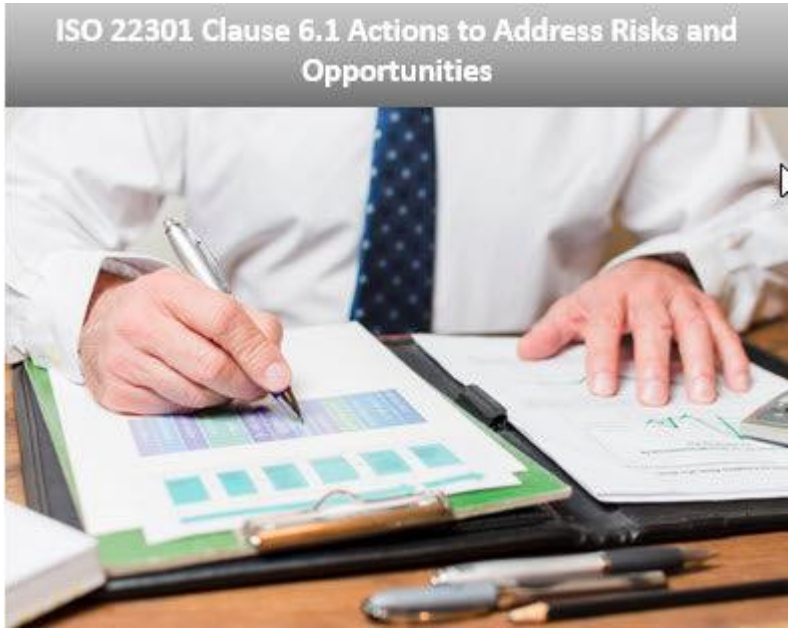
PLANIFICACIÓN Y OPERCIÓN DE LOS RIESGOS EN EL SGCN

PLANIFICACIÓN Y OPERCIÓN DE LOS RIESGOS EN EL SGCN

CONSIDERACIONES AL ANALIZAR EL RIESGOS Y LA OPORTUNIDAD

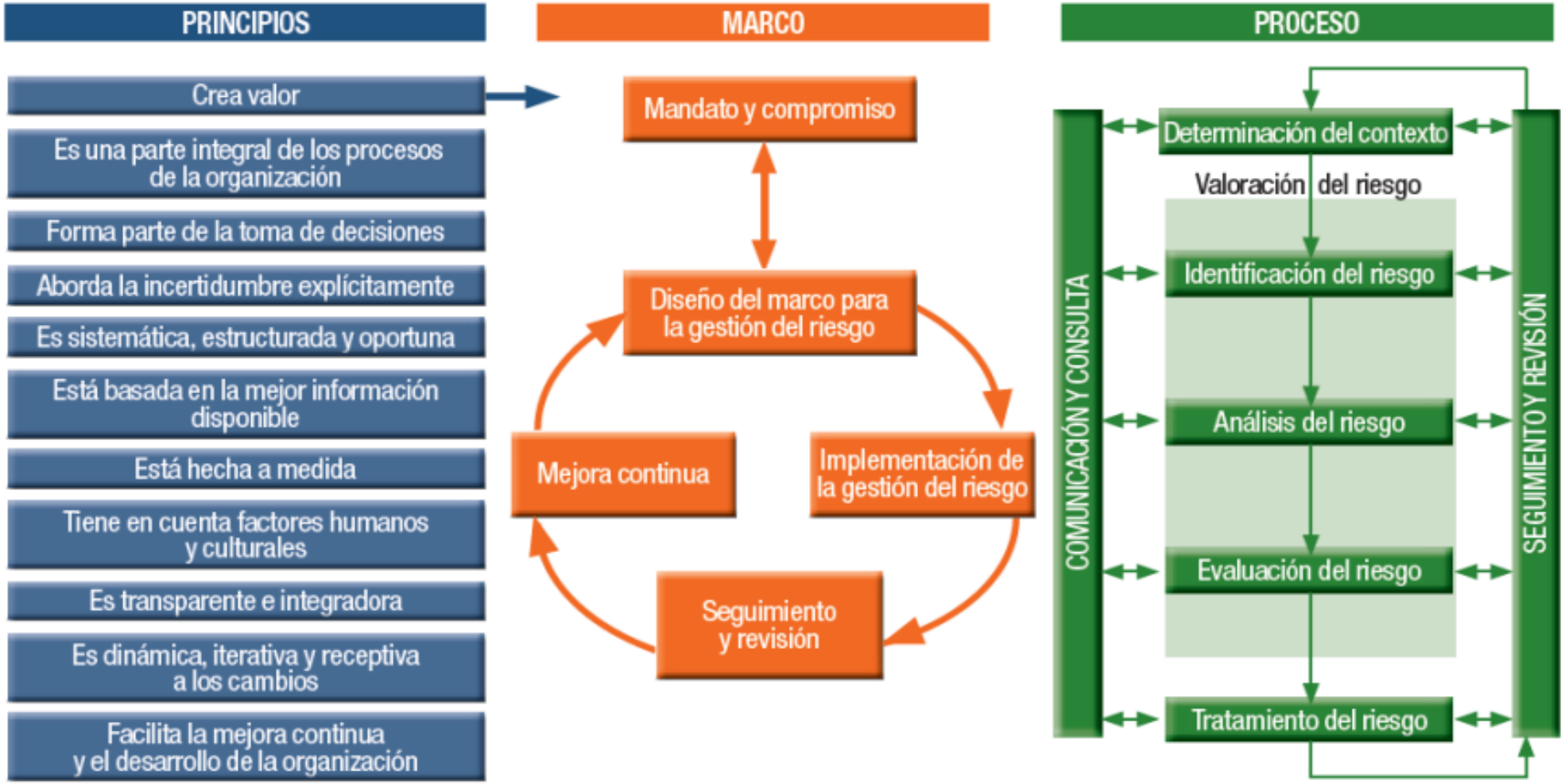
Norma ISO 22301, clausula 6.1

El pensamiento basado en riesgos es esencial para lograr un sistema en gestión de calidad eficaz. El concepto de pensamiento basado en riesgo ha estado implícito en ediciones anteriores de esta norma, incluyendo por ejemplo, llevar a cabo acciones preventivas para eliminar no conformidades potenciales, analizar cualquier no conformidad que ocurra, y tomar acciones que sean apropiadas para los efecto de la no conformidad para prevenir su recurrencia. Una organización necesita planificar e implementar acciones para abordar los riesgos y las oportunidades.



PLANIFICACIÓN Y OPERCIÓN DE LOS RIESGOS EN EL SGCN

PROCESO DE GESTIÓN DE RIESGO



ANÁLISIS Y EVALUACIÓN DE RIESGOS DEL SGCN

ANÁLISIS Y EVALUACIÓN DE RIESGOS DEL SGCN

DETERMINANDO LOS RIESGOS Y LAS OPORTUNIDADES

Norma ISO 22301, clausula 6.1.1

Al planificar el SGCN, la organización debe considerar las cuestiones referidas en el subcapítulo 4.1 y los requisitos mencionado en el subcapítulo 4.2 y determinar los riesgos y oportunidades que necesitan abordarse para:

a) Garantizar que el SGCN pueda lograr su(s) resultado(s) deseado(s).
b) Prevenir o reducir los efectos no deseados.
c) Lograr la mejora continua

ANÁLISIS Y EVALUACIÓN DE RIESGOS DEL SGCN

DETERMINANDO LOS RIESGOS Y LAS OPORTUNIDADES

Norma ISO 22301, clausula 6.1.1

Las oportunidades pueden surgir como resultado de una situación favorable para lograr un resultado previsto, por ejemplo un conjunto de circunstancias que permita a la organización atraes clientes, desarrollar nuevos productos y servicios, reducir los residuos o mejorar la productividad. Las acciones para abordar las oportunidades también pueden incluir la consideración de los riesgos asociados. El riesgo es el efecto de la incertidumbre y dicha incertidumbre puede tener efecto positivos o negativos. Una desviación positiva que surge de un riesgo puede proporcionar una oportunidad, pero no todos los efecto positivos del riesgos tiene como resultado oportunidades.

ANÁLISIS Y EVALUACIÓN DE RIESGOS DEL SGCN

ABORDANDO SOBRE LOS RIESGOS Y LAS OPORTUNIDADES

Norma ISO 22301, clausula 6.1.12

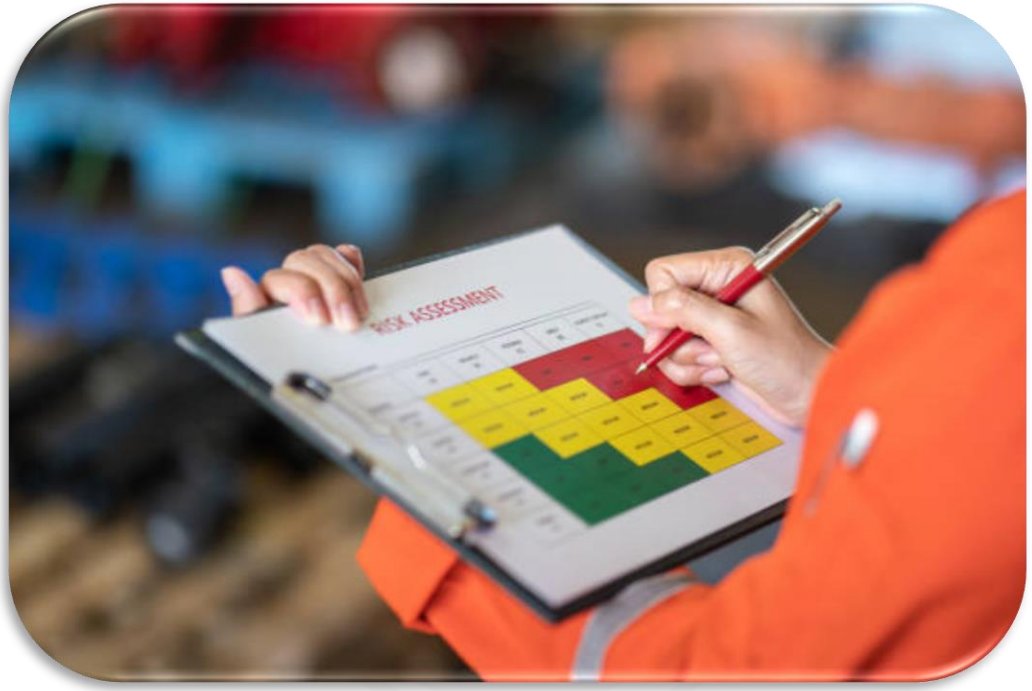
La empresa debe planificar:

a) Acciones para abordar todos los riesgos y las oportunidades
b) La manera de integrar e implementar todas las acciones de los procesos en el SGCN
c) Evaluar la eficacia de las acciones

NOTA: Los riesgos y las oportunidades se relacionan con la eficacia del sistema de gestión. Los riesgos relacionado con los disrupciones del negocio se abordan en el subcapítulo 8.2.

Ejemplo: Una organización evidencia su cumplimiento con el manual de gestión de riesgos, matriz de riesgos, mapa de riesgos.

DETERMINACION DEL CRITERIO DEL RIESGOS



DETERMINACION DEL CRITERIO DEL RIESGOS

VALORIZACION DEL RIESGO

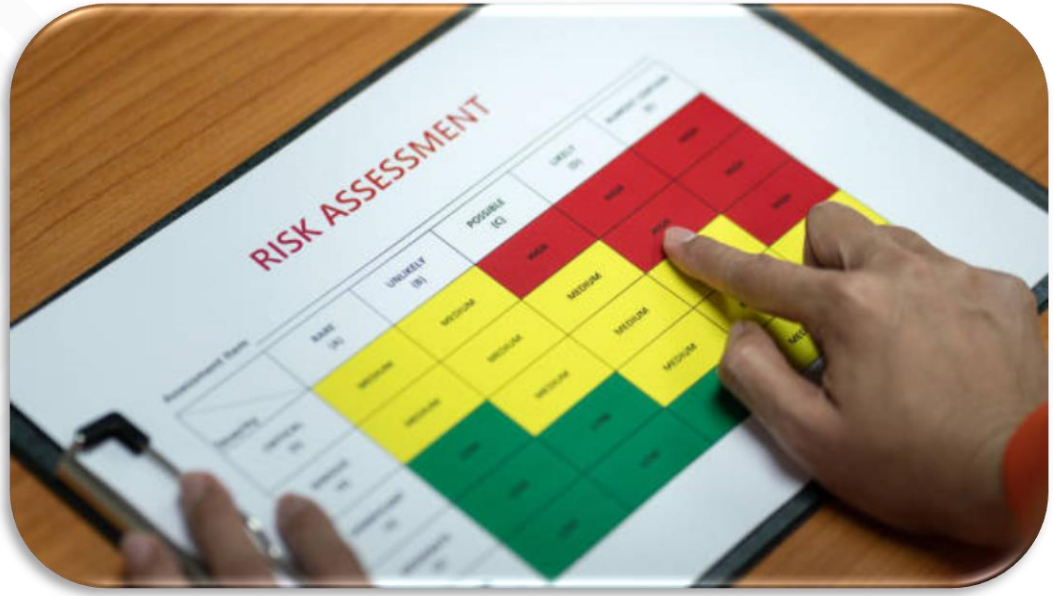
Norma ISO 22301, clausula 8.2.3

La organización deberá establecer, implementar y mantener un proceso formal documentado de evaluación de riesgos que sistemáticamente identifica, analiza y evalúa el riesgos de que se produzcan incidentes disruptivos a la organización.

NOTA: Este proceso puede ser realizado de conformidad con la norma ISO 31000:2018

La organizado debe:

- Identificar los riesgos de la interrupción en la organización de actividades prioritarias y de los procesos, los sistemas, la información, las personas, los bienes, los socios externos y otros recursos que les sirve de apoyo.
- Analizar sistemáticamente el riesgo
- Evaluar los riesgos relacionado con trastornos que requieres de tratamiento.
- Identificar los tratamientos acordes con objetivos de CN y de conformidad con el apetito por el riesgos de la organización.



DETERMINACION DEL CRITERIO DEL RIESGOS

PROTECCION Y MITIGACION

Norma ISO 22301, clausula 8.2.3

Para identificar los riesgos que requieren tratamiento, la organización deberá estudiar medidas proactivas que:

a) Reduzcan la posibilidad de una interrupción
b) Acorten el periodo de interrupción
c) Limiten el impacto de una interrupción y en la provisión de los productos y la presentación de los servicios principales de la organización.

La organización deberá elegir e implantar una tratamiento de riesgos apropiados según su nivel de aceptación del riesgo.

DETERMINACION DEL CRITERIO DEL RIESGOS

ANALISIS DE RIESGOS

El análisis de riesgos se define como el análisis de un entorno de riesgos.

Cada riesgo se evalúa de acuerdo con:

- Las perdidas que pueden ocasionar.
- La probabilidad de ocurrencia
- El costo de las contra medidas para mitigar el riesgo
- La perdida probable si esas contras medidas fueron aplicadas.

Escenario 1	Posibles Causas/Amenazas	Consecuencias	Impacto
No disponibilidad	• Fuego • Inundación • Amenaza de bomba • Huelga • Manifestación • Fuga de gas • Huracán • Terremoto	• Se ha detenido la producción • Incapacidad para garantizar la logística de entrega • Incapacidad de facturar bienes entregados	3
			Probabilidad
			2
			Nivel de Riesgo
			6

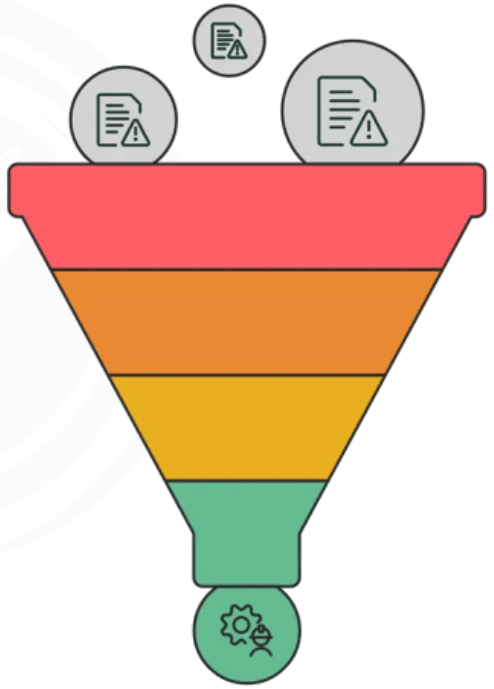
DETERMINACION DEL CRITIERO DEL RIESGO

EVALUACION DE RIESGOS

La evaluación de los riesgos es la comparación de los niveles de riesgos estimados con los criterios de evaluación y los criterios de aceptación de riesgos y priorizarlos

La estimación de riesgos es necesaria antes de tomar una decisión sobre las posibles opciones para el tratamiento de riesgos incluyendo:

- Si se tomaran medidas correctivas para reducir el nivel de riesgo calculado
- A cuales riesgos se les da prioridad.



Identificación de Riesgos
Identificar los riesgos tanto internos como externos de la organización.

Análisis de Riesgos
Evaluando la naturaleza y el impacto de los riesgos.

Valoración de Riesgos
Priorizando riesgos según su gravedad.

Tratamiento de Riesgos
Implementando medidas para mitigar riesgos.

pirani

DETERMINACION DEL CRITIERO DEL RIESGO

DECISION COMO RESULTADO DE LA EVALUACION DE RIESGOS

Las decisiones pueden incluir:

- Si un riesgo necesita tratamiento
- Prioridades de tratamiento
- Si una actividad debe llevarse a cabo
- Cual, de una cantidad de caminos debería seguirse

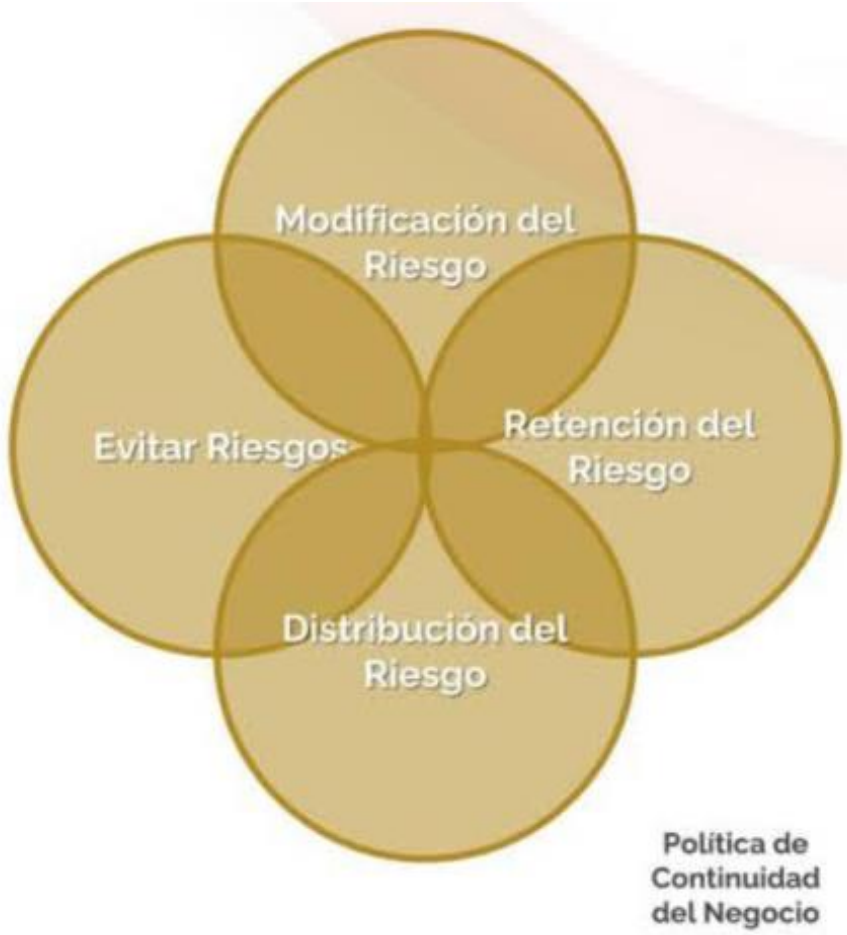
Amenaza	Valor de consecuencia (activo)	Probabilidad de ocurrencia de la amenaza	Nivel de riesgo	Orden de prioridad de la amenaza
Escenario A	5	2	10	2
Escenario B	2	4	8	3
Escenario C	3	5	15	1
Escenario D	1	3	3	5
Escenario E	4	1	4	4
Escenario F	2	4	8	3

Nota: La decisión sobre las medidas a tomar después de la evaluación del riesgo se verá influida por el nivel de apetito por el riesgo de la organización

TRATAMIENTO Y ACEPTACIÓN DEL RIESGO

TRATAMIENTO Y ACEPTACIÓN DEL RIESGO

OPCIONES DE TRATAMIENTO



Modificación del Riesgo

- Presentar, retirar o modificar los controles de modo que el riesgo residual puede ser evaluado como aceptable

Retención del Riesgo

- La dirección decidió aceptar el nivel real de riesgo

Evitar del Riesgo

- Cancelación o modificación de una actividad o conjunto de actividades relacionadas con riesgos

Distribución del Riesgo

- Decisión de compartir riesgos con las partes externas: seguro o tercerización

TRATAMIENTO Y ACEPTACIÓN DEL RIESGO

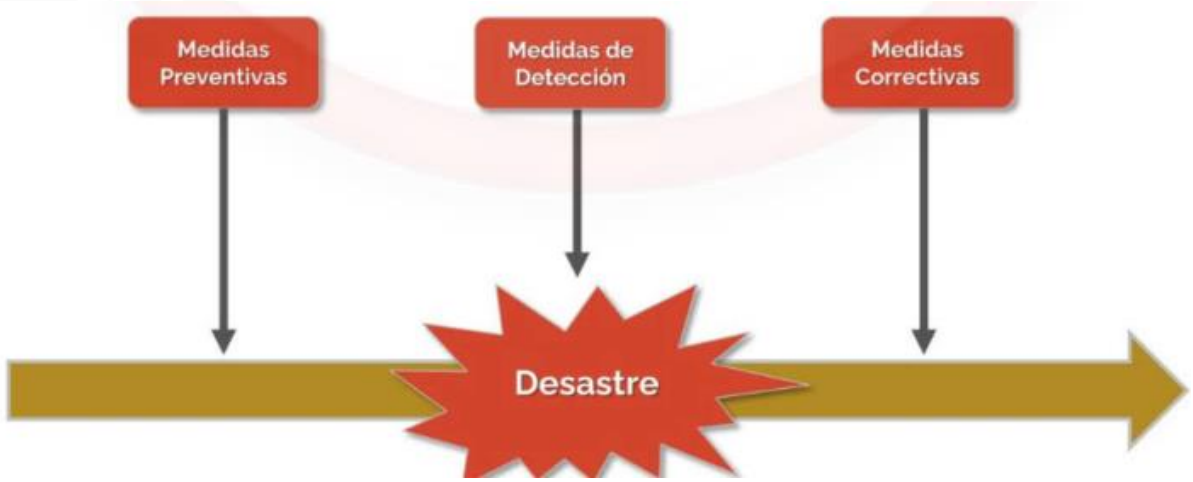
EVALUACION DE RIESGOS

Selección de medidas de protección y mitigación

- Los resultados de la evaluación de riesgos ayudaran a guiar y determinar las medidas de gestión apropiadas y las prioridades de gestión de los riesgos y para aplicar las medidas de protección y mitigación para proteger contra estos riesgos.

- Las medidas pueden ser seleccionadas a partir de varias normas o pueden diseñarse nuevos controles para satisfacer las necesidades especificas de la organización

- La selección de medidas de protección y mitigación se detallan.



TRATAMIENTO Y ACEPTACIÓN DEL RIESGO

APLICACIÓN DE MEDIDAS PREVENTIVAS

Medidas preventivas:

- Trabajar de manera proactiva
- Asegurarse de que su preparación es adecuada
- Desalentar o prevenir la aparición de problemas
- Debe estar basada sobre la mejora continua

Reducir la probabilidad y el posible impacto

- Gestión de Riesgos
- Protección física y lógica
- Gestión del cambio y de la configuración
- Mantenimiento del equipamiento

TRATAMIENTO Y ACEPTACIÓN DEL RIESGO

APLICACIÓN DE MEDIDAS DE DETECCIÓN

Medidas de detección:

- Detectar e identificar anomalías
- Dar indicación rápida
- No son discriminativas
- Deben ir seguidas de un procedimiento de escalada.

Reducir el impacto

Seguimiento

Alerta

Gestión de Incidentes

TRATAMIENTO Y ACEPTACIÓN DEL RIESGO

APLICACIÓN DE MEDIDAS DE CORRECTIVAS

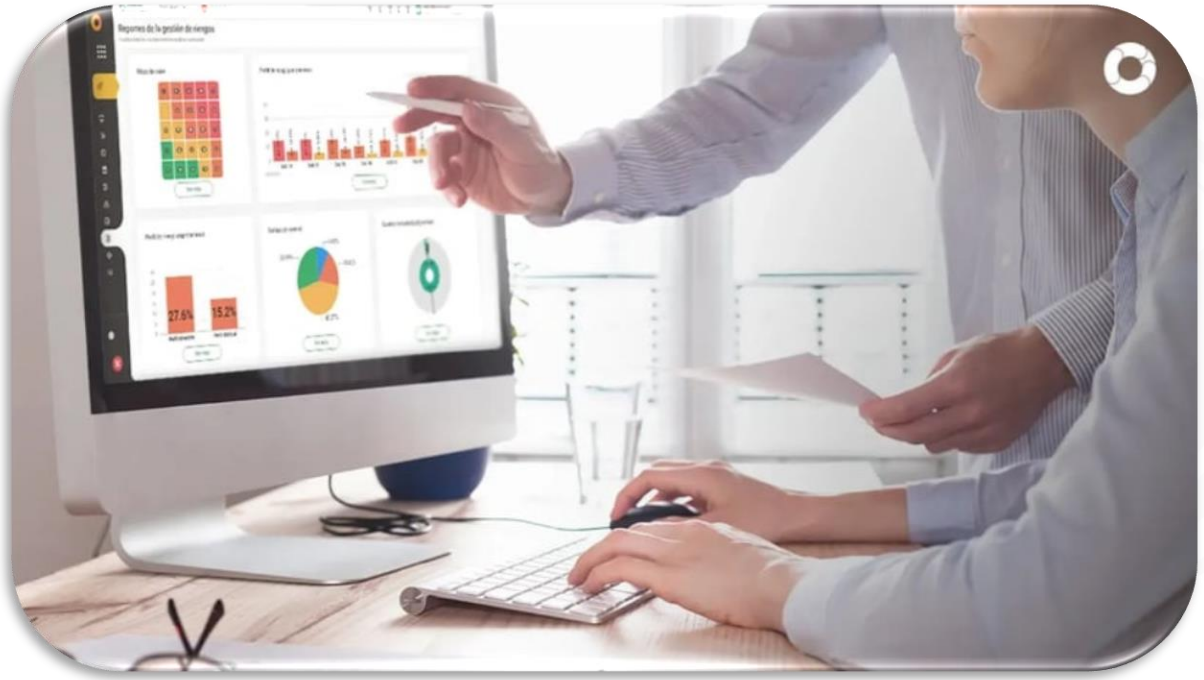
Medidas de correctivas:

- Trabajar a corto y largo plazo
- Deben seguir la gestión del cambio
- Muy probablemente necesitan la participación humana
- Deben incorporarse en la mejora continua

Mitigación de las consecuencias

- Planes de CN y RD (Recuperación ante desastres)
- Comunicación
- Copia de seguridad
- Seguimiento de No Conformidad

RIESGOS, CONTROLES Y OBJETIVOS DEL SGCN



RIESGOS, CONTROLES Y OBJETIVOS DEL SGCN

LOS OBJETIVOS Y LOS PLANES PARA ALCANZARLOS

Norma ISO 22301, clausula 6.2.
La alta dirección deberá asegurar de que los objetivos de continuidad del negocio son establecidos y comunicado para las funciones y los niveles pertinentes dentro de la organización.

Ejemplo: Una organización evidencia su cumplimiento con el documento donde se establezcan los objetivos definidos y realiza el seguimiento para su cumplimiento mediante reuniones periódicas.

RIESGOS, CONTROLES Y OBJETIVOS DEL SGCN

LOS OBJETIVOS Y LOS PLANES PARA ALCANZARLOS

Norma ISO 22301, clausula 6.2.1

La organización debe estableces objetivos de continuidad del negocio en funciones y niveles relevantes

Los objetivos de CN debe:

a) Ser coherentes con la política de continuidad del negocio
b) Ser Medibles (si es posible)
c) Tomar en cuenta los requisitos aplicables (4.1 y 4.2)
d) Ser sujetos de seguimiento
e) Ser comunicados
f) Estar actualizados según corresponda

La organización debe tener información documentada sobre los objetivos de CN.

RIESGOS, CONTROLES Y OBJETIVOS DEL SGCN

LOS OBJETIVOS Y LOS PLANES PARA ALCANZARLOS

Norma ISO 22301, clausula 6.2.2

Al planificar como lograr sus objetivos de continuidad del negocio, la organización debe determinar:

a) Lo que se hará
b) Que recursos se requerirán
c) Quien será responsable
d) Cuando se completara
e) Como se evaluaran los resultados.

¡Gracias!

Centro de
Especializaciones
Noeder

Conéctate con nuestra comunidad

© 2026 | CENTRO DE ESPECIALIZACIONES NOEDER | R.U.C. 20604924236 | Todos los derechos reservados